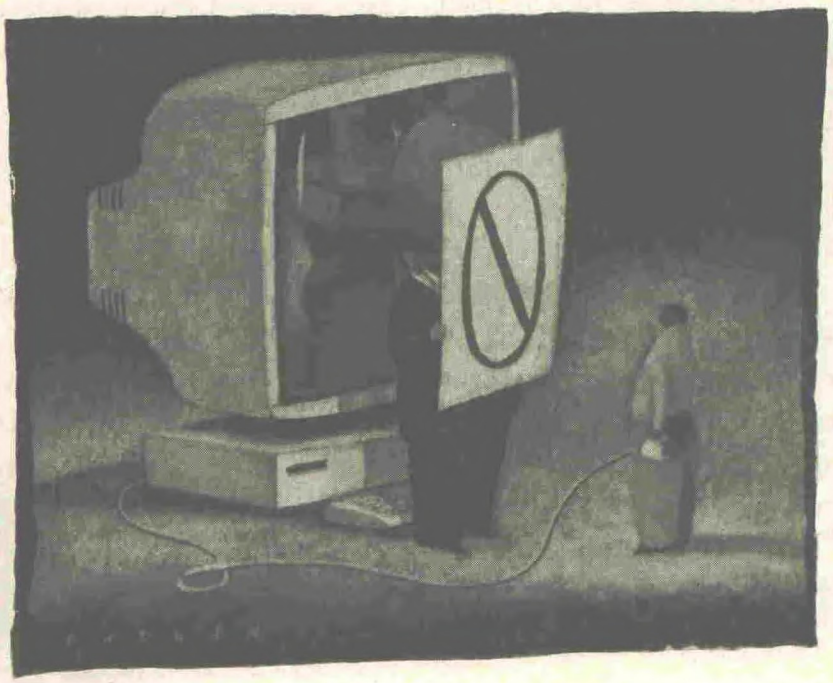
ดร. อนุชา พิทักษานนท์กุล

เทคนิคการสร้างความปลอดภัยแก่เวบไซท์

อธิบายถึงการที่พวกแฮกเกอร์ใช้เทคนิคต่าง ๆ ในการเจาะเข้าไปในระบบเครือข่าย เป็นเทคนิคใหม่ที่เกิดขึ้นไม่นานมานี้



ท่านทราบไหมว่าในแต่ละวินาทีที่ผ่านไปมีคนจ้องที่จะเจาะเข้าไปในเวบไซท์ของท่านอยู่ตลอดเวลา กลุ่มบุคคลที่ใช้เวลาและความพยายามในการที่จะล้วงข้อมูลจากโฮสต์ (host) ของท่านนั้นมีทั้งนักวิชาการ นักคอมพิวเตอร์สมัครเล่น กลุ่มมิจฉาชีพ ตลอดจนเด็กวัยรุ่นที่ชอบที่จะเป็นแฮกเกอร์ ซึ่งจะนั่งอยู่หน้าจอคอมพิวเตอร์ตลอดทั้งวันทั้งคืนเพื่อค้นหา พาสเวิร์ด (password) ของท่านเพื่อล้วงลึกเข้าไปในคอมพิวเตอร์ต่อไป การเจาะทะลุระบบอินเทอร์เน็ตโดยเฉพาะตัวคอมพิวเตอร์ UNIX ที่เป็นโฮสต์นั้นสามารถทำได้ง่ายมากถ้าท่านไม่มีการป้องกันไว้อย่างเพียงพอ ระบบ เวิร์ลไวด์เวบ (WWW) เป็นระบบที่ได้รับความนิยมเป็นพลุแตกเลยก็ว่าได้ ในช่วงระยะเวลาปีถึงสองปีที่ผ่านมา บริษัทและหน่วยงานใหญ่ ๆ ทั่วโลกต่างก็มีโฮมเพจของตัวเอง เพื่อใช้ในการเผยแพร่ข่าวสารของบริษัท ตลอดจนถึงขายของผ่านระบบอินเทอร์เน็ตกันเลยทีเดียว อย่างไรก็ตาม ตัวเวิร์ลไวด์เวบถือได้ว่าเป็นจุดอ่อนจุดหนึ่งของระบบอินเทอร์เน็ต เพราะจุดประสงค์ของมันก็คือต้องการให้คนเข้ามาอ่านโฮมเพจ ซึ่งก็ต้องอยู่บนฮาร์ดดิสค์บนเครื่องที่เป็นโฮสต์ของเรา การที่คนเข้ามาถึงฮาร์ดดิสค์ของเราได้ก็นับว่าหมิ่นเหม่ต่อการที่เขาจะวิ่งไปที่ส่วนอื่นได้เช่นเดียวกัน ทีนี้ถ้าเราพลั้งเผลอไม่ป้องกันให้ดีพอก็อาจถูกล้วงตับได้ง่าย ๆ เหมือนกัน

บทความนี้จะพูดถึงความปลอดภัยของระบบอินเทอร์เน็ต และยูนิกซ์โฮสต์ การป้องกันไม่ให้คนเข้ามาข้อมูลเราได้ พวกแฮกเกอร์ใช้วิธีอย่างไรในการเจาะไซท์ของเรา เราจะสู้กับพวกแฮกเกอร์หรือพวกนักวิชาการใต้ดินเหล่านี้ได้อย่างไร

ดมกลิ่นหารหัสผ่าน (Password Sniffing)

วิธีการที่ง่ายที่สุดในการเจาะผ่านเข้าระบบอินเทอร์เน็ตก็คือการค้นหารหัสผ่านหรือพาสเวิร์ด ถ้าท่านเคยใช้อินเทอร์เน็ตคงพอจะจำได้ว่าท่านจะต้องพิมพ์ชื่อ (User Name) และรหัสผ่านจึงจะเข้าไปในระบบได้ ดังนั้นถ้าท่าน

ใช้ชื่อไม่ดีพอ เช่น JOE และใช้รหัสผ่านว่า JOE123 ก็อาจจะมีคนพิมพ์ชื่อ JOE และลองพิมพ์รหัสผ่าน JOE1, JOE2, JOE 3.... ไปเรื่อย ๆ จนถึง JOE123 ก็จะเข้าระบบได้ การลองแบบนี้ถ้ามีเวลาพอก็อาจจะนั่งพิมพ์ไปเรื่อย ๆ จนกว่าจะเจอ หรือใช้โปรแกรมช่วยหาก็ได้ โปรแกรมประเภทนี้จะเป็นประเภทที่เราเรียกว่าใช้กำลังและความอดทนในการหา (Brute Force) คือมันจะลองหาอย่างไม่มีเหนื่อยไม่มีเหนื่อยจนกว่าจะเจอ หรือไม่ก็ลองหาเรื่อยไปไม่มีวันหยุด

การหารหัสผ่านอีกแบบที่นิยมกันมากก็คือดูที่ไฟล์ชื่อ /etc/passwd ซึ่งในระบบยูนิกซ์รุ่นเก่าที่ยังไม่ใช้รหัสผ่านเงา (shadow password) ก็จะเก็บชื่อและรหัสผ่านไว้ในนี้ทั้งหมด พวกแฮกเกอร์สามารถใช้โปรแกรมค้นหาเช่น CRACK เพื่อค้นหารหัสผ่านจากไฟล์นี้ได้

ในระบบยูนิกซ์รุ่นใหม่ ๆจะใช้รหัสผ่านเงา ซึ่งจะทำให้การค้นหารหัสผ่านทำได้ยากขึ้น

ตัวอย่างของรายชื่อใน /etc/passwd

```
root:x:0:1:Sys. Admin:/:/bin/sh
```

โดยที่ตรงตำแหน่งตัว x จะเป็นพาสเวิร์ดที่มีการเข้ารหัสไว้แล้ว และพาสเวิร์ดที่เข้ารหัสไว้แล้วนั้นจะเก็บไว้ในไฟล์ชื่อ /etc/shadow ซึ่งแต่ละแถวในนั้นจะมีรูปร่างหน้าตาดังนี้

```
root:XyfgFekj95Fpq:::::
```

ซึ่งจะเก็บข้อมูลเกี่ยวกับชื่อและรหัสผ่าน รวมทั้งข้อมูลอื่น ๆ เช่น อายุของรหัสผ่านเป็นต้น การเก็บรหัสผ่านไว้ใน /etc/shadow นี้ทำให้การถอดรหัสผ่านนั้นยากขึ้น แต่ก็ไม่ใช่ว่าจะทำไม่ได้เสียเลย อย่างเช่นในระบบ SUNOS ซึ่งจะเก็บข้อมูลเกี่ยวกับรหัสผ่านไว้ในไฟล์ชื่อ /etc/security/passwd.adjunct และผู้ที่จะอ่านไฟล์นี้ได้ต้องเป็นรูท (root) เท่านั้น ดังนั้นเราจึงไม่สามารถใช้วิธีบรูทฟอร์ซได้ โปรแกรมอย่างเช่น CRACK ก็ไม่สามารถสกัดรหัสผ่านได้เช่นกัน เราลองมาดูตัวอย่างของ /etc/passwd ของ SUNOS ที่ใช้ระบบรหัสผ่านเงา ซึ่งจะมีรูปร่างหน้าตาดังนี้

```
root:##root:0:1:System
Administrator:/:/bin/csh
```

การที่แฮกเกอร์ไม่สามารถใช้โปรแกรม CRACK ได้ก็ไม่ใช่ว่าไซท์ของท่านจะไม่ถูกเจาะ เทคนิคหนึ่งที่กำลังฮิตกันอยู่ในตอนนี้ก็คือ การใช้ฟังชันที่ชื่อว่า pwdauth() ซึ่งจะรับชื่อและรหัสผ่านเข้าไปในตัวฟังก์ชัน จากนั้นมันจะเข้ารหัสเจ้าตัวพาสเวิร์ดแล้วไปเปรียบเทียบกับที่เก็บในรหัสผ่านเงา ซึ่งถ้าเจอตรงกันก็จะทำให้แฮกเกอร์รู้ได้ทันทีว่า นี่คือรหัสผ่านที่ใช้ได้

IP Spoofing

ไอพี สปูฟฟิ่ง มีชื่อเสียงโด่งดังขึ้นมาก็ตอนที่ยอดชายนายเควิน มิทนิค แฮกเกอร์คนดังใช้วิธีนี้ในการเจาะเข้าไปในบริษัทโนเวลซัน เน็ทคอม และอีกหลาย ๆ มหาวิทยาลัยในสหรัฐอเมริกา ไอพี สปูฟฟิ่ง มีวิธีการทำงานดังนี้

ขั้นแรกเจ้าแฮกเกอร์ก็จะติดตั้งโฮสต์ที่ดูเสมือนโฮสต์จริง ๆ ในระบบอินเทอร์เน็ต แต่จะใช้เลขไอพี (IP address) ปลอม ที่เป็นเลขไอพีที่ดูเหมือนเป็นมิตรไม่ใช่ศัตรู ซึ่งก็จะหลอกตัวกำแพงไฟ (firewall) โดยเฉพาะกำแพงไฟแบบแค่กรองเลขไอพี ให้เจ้าเครื่องที่ใช้ไอพีปลอมของเจ้าแฮกเกอร์ผ่านไปได้ แต่กำแพงไฟแบบในระดับชั้นแอพพลิเคชันจะจับได้และไม่ให้เจ้าไอพีหลอก ๆ นี้ผ่านไปได้

Web Spoofing

ที่กำลังมาแรงในตอนนี้ก็คือวิธีที่เรียกว่า เวบ สปูฟฟิ่ง โดยที่เจ้าแฮกเกอร์ก็จะจัดตั้งเวบไซท์ปลอม ๆ ขึ้นมาแล้วก็ทำการขายของหลอก ๆ ดังนั้นใครหลงเข้าไปซื้อของโดยเฉพาะการใช้เครดิตการ์ดในการซื้อของก็จะถูกขโมยเบอร์เครดิตการ์ดไปได้อย่างง่ายดาย ถ้าท่านต้องการรายละเอียดมากขึ้น ท่านสามารถหาข้อมูลเพิ่มเติมได้จาก

```
www.cs.princeton.edu
```

มีแฮกเกอร์หัวใสรายหนึ่งตั้งเวบไซท์ชื่อ MICROSOFT.com ขอให้ท่านสังเกตว่าเขาใช้เลข ศูนย์ แทนที่ตัวโอ ซึ่งก็จะมีผู้ใช้อินเทอร์เน็ตอยู่มากมายเข้าไปที่ไซท์นี้แล้วเกิดความสับสนว่าเป็นไซท์ของไมโครซอฟท์จริง ๆ อันนี้ก็เป็นเรื่องน่าเป็นห่วงเพราะว่าผู้ใช้อินเทอร์เน็ตที่ไม่มีความรอบคอบอย่างเพียงพอก็จะถูกหลอกอย่างง่ายดาย เพราะเจ้าเวบไซท์หลอกนี้สามารถไปดึงข้อมูลจริง ๆ จากเวบไซท์ของไมโครซอฟท์มาแสดงทำทีว่าเป็นไมโครซอฟท์ตัวจริงก็ได้เช่นกัน แต่ในระหว่างนั้นก็อาจจะหลอกถามข้อมูลสำคัญจากลูกค้าไปเสียแล้ว เพราะฉะนั้นถึงแม้ว่าท่านจะใช้ SSL (Secure Sockets Layer) ที่ตัวบราวเซอร์ก็ไม่ช่วยอะไรได้ เพราะเจ้าเวบไซท์เป็นผู้ร้ายไปซะเอง หนทางป้องกันก็อาจจะต้องหาทางให้ตัวบราวเซอร์กับตัวเซอร์ฟเวอร์คุยกันเสียก่อนว่าเป็นตัวจริงทั้งคู่ ไม่ใช่ตัวปลอมที่ด้านใดด้านหนึ่ง ตัวอย่างเช่น ซอฟต์แวร์ชื่อ เวบครูเสดเดอร์ ของบริษัทเกรเดียนท์ ที่สามารถเช็คข้อมูลอันนี้ได้ และก็ยังมีความสามารถในด้านลายเซนต์ดิจิตอลด้วยเช่นกัน ก็พอจะป้องกันไปได้บ้าง

นักวิจัยที่มหาวิทยาลัยปริ๊นซตันแนะนำให้ท่านปลดความสามารถในการเล่นจาวาสคริปต์ออกจากตัวเน็ตสเคป เพื่อที่ว่าถ้ามีแฮกเกอร์รายใดโจมตีไซท์ของท่าน ท่านก็สามารถค้นหาร่องรอยได้บ้าง ถ้ามีจาวาสคริปต์อยู่เจ้าแฮกเกอร์ก็อาจจะใช้จาวาสคริปต์ในการกลบร่องรอยในการลอบเข้ามาในเครื่องเราได้ นอกเหนือจากนั้นเวลาท่านเล่นเน็ตสเคปอยู่ก็ให้คอยสังเกตว่าในช่องโลเคชันนั้นเป็นจุดที่ท่านต้องการจะไปจริง ๆ ไม่ใช่ถูกนำไปโดยที่ท่านไม่รู้ตัวหรือเป็นไซท์ปลอม

จุดอ่อนของCGI

CGI (Common Gateway Interface) เป็นวิธีการที่ตัวบราวเซอร์สามารถรับข้อมูลจากผู้ใช้ เช่น ให้ผู้ใช้พิมพ์ชื่อ นามสกุลเข้าไป จากนั้นตัวบราวเซอร์ก็ทำการส่งข้อมูลที่รับเข้ามานี้ไปยังตัวเวบเซอร์ฟเวอร์ ซึ่งตัวเวบเซอร์ฟเวอร์ก็จะรับข้อมูลแล้วสามารถเรียก

โปรแกรมที่เรียกว่า CGI Script ขึ้นมาประมวลผลข้อมูลนี้ได้

```
<A HREF=
"http://absolut.sites.uiuc.edu/
cgi-example.cgi">Click Here</A>
```

ในที่นี้ตัว CGI Script คือ cgi-example.cgi ซึ่งรายละเอียดจะอยู่ในลิสติงที่ 1 เมื่อผู้ใช้คลิ๊กที่บรรทัดนี้ ตัวบราวเซอร์ก็จะส่งข้อมูลไปยังตัวเซอร์ฟเวอร์ ตัวเซอร์ฟเวอร์ก็จะรับข้อมูลและเรียกโปรแกรม cgi-example.cgi ขึ้นมาทำงาน จุดอ่อนของ CGI ก็คือว่ามันจะทำงานโดยไม่สนใจว่าคนที่มาเรียกโปรแกรมนั้นเป็นมิตรหรือเป็นศัตรู กรณีที่เป็นข่าวขึ้นมาก็เกี่ยวข้องกับ PHF (Packet Handling Function) โปรแกรมของตัว CGI Script ตัว PHF เป็นตัวอย่างโปรแกรมที่ใช้สอนการเขียนโปรแกรม CGI ซึ่งก็อาจเป็นโปรแกรมที่ใช้ค้นหาข้อมูลจากออเรเคิล หรืออินฟอร์มิกซ์ หรือฐานข้อมูลตัวอื่น ๆ ก็ได้

จากที่ได้อธิบายไปแล้วว่า CGI Script เป็นโปรแกรมที่ใครเข้ามาเรียกใช้งานก็ได้ ดังนั้นถ้าเจ้าแฮกเกอร์รู้ช่องโหว่ตรงนี้ ก็ใช้ PHF ไปดึงเอาไฟล์ /etc/passwd และ /etc/shadow ออกมา จากนั้นใช้โปรแกรมดมกลิ่นรหัสผ่านที่ได้อธิบายไปแล้วในตอนต้นของบทความ ก็จะสามารถถอดรหัสผ่านของใครคนหนึ่งหรือกระทั่งของรูทออกมาจนได้ ซึ่งก็จะทำให้เจาะลึกเข้าไปในโฮสต์ได้มากขึ้น เหตุการณ์นี้มีรายงานแล้วว่าเกิดขึ้นจริงกับบริษัทชื่อ ไซเบอร์ซิสเต็ม ในรัฐนอร์ทแคโรไลน่า ประเทศสหรัฐอเมริกา โดยที่เจ้าแฮกเกอร์เมื่อเจาะเข้าไปในโฮสต์ได้แล้วก็เพียงแต่ดัดแปลงโฮมเพจของบริษัทเท่านั้น ยังไม่ถึงกับทำอันตรายอะไร

ลิสติงที่ 1 ตัวอย่าง cgi-example.cgi

```
#!/usr/bin/perl
### We need this file to load the ENV info, and process form input
### (no form input is here in this example)
require "cgi-lib.pl";
### This library has the ctime() function

require "ctime.pl";

### This is the function in cgi-lib.pl that reads ini info and puts it into
### 2 associative arrarys, %in for form input, and %ENV for browser/misc info
&ReadParse;
### Every script MUST print these two lines first or it won't work
print "Content-type: text/html\n";
print "\n";
### Some normal html
### Note that a quote must be escaped ( \" instead of just " ) since perl
### would think you were ending the print command otherwise
print "<center>";
print "<body BGCOLOR = \"#000000\" LINK = \"#A0D0D0\" TEXT = \"#FFFFFF\" VLINK = \"#A0D0D0\"
ALINK = \"#A0D0D0\">";
print "<html>";
print "<title> An example cgi script </title>";
### One of the things in %ENV are IP names and numbers
$ipname = $ENV{'REMOTE_HOST'};
$ipnum  = $ENV{'REMOTE_ADDR'};
print "Your ip address is <br>\n";
if($ipname eq "") {
    print "<h2>$ipnum</h2>\n";
} else {
   print "<h2>$ipname</h2>\n";
}
### Get the date string and remove the newline at the end, if there is one
$thetime = &ctime(time);
chomp($thetime);
###
### Lets log the date of when the page was accessed
###
if(open(LOGME, ">>enter.log")) {
   print LOGME "Hit at $thetime\n";
   close LOGME;
}
## seed the random number generator with the time
srand(time);
$random = int(rand(10000));
print "Your lucky number is $random\n<p>\n";
print "<a href=\"cgi-example.txt\"> The source for this program </a>\n";
exit;
```

ช่องโหว่เหล่านี้เกิดขึ้นเพราะ CGI Script มักจะไม่ได้เขียนโดยคนที่มีความรู้ในด้านความปลอดภัยของคอมพิวเตอร์และอินเทอร์เน็ตดีพอ มักจะเขียนโดยกราฟิกดีซายเนอร์ หรือโฮมเพจดีซายเนอร์ที่อาจจะไม่เข้าใจสถาปัตยกรรมของคอมพิวเตอร์ที่เป็นเวบเซอร์ฟเวอร์อย่างถ่องแท้ และยิ่งไปกว่านั้นก็คือ ใคร ๆ ก็อยากเขียน CGI Script โดยคิดว่านั่นคือสุดยอดของการสร้างโฮมเพจ ดังนั้นผู้บริหารควรให้ความสนใจในจุดนี้ด้วย ต้องให้การศึกษาที่ถูกต้องกับบุคลากรที่จะมานั่งเขียน CGI Script เพราะว่าถ้าเขียนแล้วไม่มีความปลอดภัยก็จะเป็นช่องโหว่ช่องใหญ่ที่ให้คนเข้ามาล้วงข้อมูลในบริษัทท่านได้

ไอเอสพีจงระวังน้ำท่วม

สิ่งหนึ่งที่ไอเอสพี (ISP-Internet Service Provider) กลัวที่สุดก็คือถูกแกล้งให้ดูเสมือนว่าให้บริการที่ยอดแย่ โดยที่เจ้าแฮกเกอร์จะหมุนโทรศัพท์เข้ามาทำให้สายมันไม่ว่างเสียอย่างนั้นแหละ และก็ยังทำให้เครือข่ายของสายโทรศัพท์มันอุดตันเสียเล่นๆ การเข้าโจมตีของแฮกเกอร์ในลักษณะนี้จะเรียกว่า การโจมตีแบบ เอสวายเอ็นฟลัดดิ้ง (Synchronized Number Sequence Flooding) ซึ่งบริษัทที่โดนก็มีเน็ทคอม ซึ่งเป็นไอเอสพีรายใหญ่รายหนึ่งของประเทศสหรัฐอเมริกา รวมทั้งบริษัทแพนิกซ์ และรายย่อย ๆ อีกหลายราย โดยการโจมตีนี้ทำให้บริการของบริษัทเหล่านี้ถึงกับเป็นง่อยไปเลยทีเดียว ข่าวดีของการโจมตีแบบนี้ก็คือตัวแฮกเกอร์ยังเจาะเข้าไปไม่ถึงตัวคอมพิวเตอร์หรือตัวโฮสต์ เพียงแต่ทำให้เครือข่ายพิการไปเท่านั้นเอง

แฮกเกอร์โจมตีโดยการปลอมไอพีแอดเดรสต้นทาง บนเอสวายเอ็นแพคเกจ ซึ่งก็คือเป็นตัวแพคเกจที่ใช้สำหรับการซิงโครไนเซชันของการเดินทางของตัว TCP เจ้าแฮกเกอร์ก็จะโจมตีโฮสต์เป้าหมายนี้ไปเรื่อย ๆ ซึ่งโดยทั่ว ๆ ไปแล้วตัวโฮสต์จะรองรับช่องการสื่อสารได้ประมาณ 8 ถึง 16 ช่องของการติดต่อสื่อสาร ตัวเครือข่ายจะเปิดช่องเพื่อการติดต่อสื่อสารในกรณีมีการส่งข้อมูลระหว่างเครื่อง ดังนั้นถ้ามีการส่งข้อมูลโดยการใช้ไอพีแพคเกจปลอม เจ้าไอพีแพคเกจปลอมนี้ก็จะยึดช่องสื่อสารไปหมด โดยที่ไอพีแพคเกจตัวจริงไม่มีโอกาสติดต่อเข้ามาได้ บริษัทแพนิกซ์ซึ่งโดนการโจมตีแบบนี้รายงานว่า ในระหว่างการโดนโจมตีมีจำนวนแพคเกจปลอม 150 แพคเกจต่อวินาทีเข้ามาที่เครือข่ายของบริษัท และแพคเกจปลอมเหล่านี้ก็ยังใช้เลขไอพีเปลี่ยน ๆ ไปด้วย ซึ่งเป็นการยากในการตรวจสอบ บริษัทแพนิกซ์ใช้เวลาถึง 2 อาทิตย์ในการแก้ปัญหาจากการโจมตี วิธีหนึ่งที่บริษัทแพนิกซ์ทำก็คือขยายจำนวนช่องการสื่อสารและลดช่วงเวลานอกของช่องการสื่อสาร ซึ่งจะทำให้ช่องการสื่อสารไม่อุดตันจากแพคเกจปลอม บริษัทแพนิกซ์ยังดำเนินการติดตั้งโปรแกรมเพิ่มเติมที่ตัวซิสโก้เราเตอร์ ที่คอยดักและเช็คว่าทีซีพีแพคเกจที่เข้ามานั้นเป็นตัวปลอมหรือตัวจริง การแก้ปัญหาระยะยาวของไอเอสพีก็คือต้องกรองแพคเกจที่ส่งออกไป โดยจะต้องมั่นใจว่าไม่มีแพคเกจปลอมวิ่งอยู่ในเครือข่าย

ตายด้วยโปรแกรมปิง (Ping o' Death)

ในกรณีนี้ตัวโฮสต์สามารถถูกทำให้ตายหรือแครช (Crash) หรือถูกรีบูธได้โดยการส่งข้อมูลด้วยโปรแกรมปิง (Ping) ที่มีขนาดข้อมูลใหญ่กว่า 65,536 ไบต์ ซึ่งการส่งข้อมูลโดยโปรแกรมปิงนั้นปกติจะส่งแค่ 64 ไบต์ ถ้าส่งข้อมูลที่มีขนาดใหญ่เกินไปและไม่มีการเช็คก็อาจทำให้เครื่องตายได้ ทางแก้ก็คือต้องให้เราเตอร์สามารถเช็คข้อมูลปิงที่มีขนาดใหญ่เกินไปได้ หรือท่านอาจตั้งกำแพงไฟ (firewall) แล้วก็กรองข้อมูลปิงที่ตัวกำแพงไฟ ก็สามารถป้องกันได้

DNS Hijaking

การโจมตีแบบนี้เมื่อเทียบไปแล้วเป็นการโจมตีแบบเบา วิธีการก็คือเจ้าแฮกเกอร์จะเปลี่ยนทิศทางของข้อมูลจากโดเมนหนึ่งไปยังอีกโดเมนหนึ่ง เช่น จาก WWW.Yahoo.com ไปยัง www.webcolor.com อันนี้ก็คล้าย ๆ กับการเปลี่ยนเลขหมายโทรศัพท์ที่ yahoo ด้วยเลขหมายโทรศัพท์ของ webcolor ดังนั้นถ้าเราจะโทรไปที่ yahoo ก็จะไปติดที่ webcolor ทุกที การโจมตีแบบนี้เป็นการทำที่ง่ายกว่าเวบ สปูฟฟิ่งมาก และเจ้าของตัวจริงอย่างเช่นของ yahoo ก็ไม่สามารถทำอะไรได้ด้วย แต่วิธีนี้ก็ยังเป็นเพียงแต่แกล้งกันสถานเบาเท่านั้นเอง

สรุป

บทความนี้ได้อธิบายถึงการที่พวกแฮกเกอร์ใช้เทคนิคต่าง ๆ ในการเจาะเข้าไปในระบบเครือข่ายของบริษัทของท่าน เทคนิคต่าง ๆ ในบทความนี้จะเป็นเทคนิคใหม่ที่เกิดขึ้นไม่นานมานี้ ส่วนท่านที่สนใจวิธีการดั้งเดิม เช่นการเจาะโดยใช้โปรแกรม sendmail หรือ ftpd สามารถค้นคว้าเพิ่มเติมได้จากหนังสืออ้างอิงท้ายบทความ

เอกสารอ้างอิง

1. UNIX System Security A Guide for Users and System Administrators โดย David A. Curry สำนักพิมพ์ Addison-Wesley

2. Practical UNIX Security โดย Simson Garfinkel และ Gene Spafford สำนักพิมพ์ O'Reilly & Associates, Inc.